UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/680,965	10/07/2003	William J. Crilly JR.	1959-9	6070

81178 7590 06/22/2010

Daniel P. Burke, Esq.
Daniel P. Burke & Associates, PLLC
240 Townsend Square
Oyster Bay, NY 11771

EXAMINER	
POWERS, WILLIAM S	

ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
06/22/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/680,965	CRILLY, WILLIAM J.	
	Examiner	Art Unit	
	WILLIAM S. POWERS	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 November 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-80* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-80* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 11/20/2009 have been fully considered but they are not persuasive.

2. As to Applicant's argument that, "Harvey et al. does not teach this as part of an approach with a focus being placed on profiling the signal characteristic of signals from a single source address, with the specific intent of detecting wireless interlopers" (Remarks, p. 18), the Examiner respectfully disagrees. Applicant is directed to [0107-0108] of Harvey which specifically mentions analyzing signals from the same MAC address to ensure that unauthorized users are not spoofing an authorized MAC address. This reads on detecting wireless interlopers (unauthorized users) and a single source address (MAC address). As can also been seen in the Abstract of the Harvey application, the purpose of the Harvey method and system is to detect the presence of unauthorized users (Harvey, Abstract). It is also noted that Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. For at least the reasons above, the rejection of the limitations is maintained.

3. As to Applicant's argument that, "Harvey et al. does not teach the use of such an access station or remote as part of an approach with a focus being placed on profiling

the signal characteristic of signals from a single source address, with the specific intent of detecting wireless interlopers" (Remarks, p. 18), the Examiner respectfully disagrees. The Applicant is directed to the Abstract of the Harvey application, the purpose of the Harvey method and system is to detect the presence of unauthorized users (Harvey, Abstract) and, as such, the components of Harvey are integral to the system and method of increasing wireless network security. Applicant is also directed to [0107-0108] of Harvey which specifically mentions analyzing signals from the same MAC address to ensure that unauthorized users are not spoofing an authorized MAC address. This reads on detecting wireless interlopers (unauthorized users) and a single source address (MAC address). It is also noted that Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. For at least the reasons above, the rejection of the limitations is maintained.

4. As to Applicant's argument that, "Harvey et al. does not teach the use of such an antenna array as part of an approach with a focus being placed on profiling the signal characteristic of signals from a single source address, with the specific intent of detecting wireless interlopers" (Remarks, p. 18), the Examiner respectfully disagrees. The Applicant is directed to the Abstract of the Harvey application, the purpose of the Harvey method and system is to detect the presence of unauthorized users (Harvey, Abstract) and, as such, the components of Harvey are integral to the system and method of increasing wireless network security. Applicant is also directed to [0107-

0108] of Harvey which specifically mentions analyzing signals from the same MAC address to ensure that unauthorized users are not spoofing an authorized MAC address. This reads on detecting wireless interlopers (unauthorized users) and a single source address (MAC address). It is also noted that Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. For at least the reasons above, the rejection of the limitations is maintained.

5. As to Applicant's argument that, "the teachings of Harvey et al., only includes a system for detecting various locations of the device. The reference does not teach a monitoring action comprising ascertaining that at least one signal characteristic for the plurality of signals, and certainly not as part of an approach that profiles the signal characteristics from a single source address, with the specific intent of detecting wireless interlopers" (Remarks, p. 18), the Examiner respectfully disagrees. Applicant is directed to [0107-0108] of Harvey which specifically mentions analyzing signals from the same MAC address to ensure that unauthorized users are not spoofing an authorized MAC address. This reads on detecting wireless interlopers (unauthorized users) and a single source address (MAC address). The system detects the physical locations of the signals which reads on a signal characteristic and if the physical locations of the signals from the same MAC address exceed a threshold, an alert is raised that an authorized user may be on the network. For at least the reasons above, the rejection of the limitations is maintained.

6. As to Applicant's argument that, "Harvey et al. does not teach the use of signal strength and location triangulation for arrival direction as part of an approach with a focus being placed on profiling the signal characteristic of signals from a single source address, with the specific intent of detecting wireless interlopers" (Remarks, p. 19), the Examiner respectfully disagrees. Applicant is directed to Harvey [0042] in which signal strength and triangulation as well as other characteristics are used in uncovering unauthorized users. Applicant is directed to [0107-0108] of Harvey which specifically mentions analyzing signals from the same MAC address to ensure that unauthorized users are not spoofing an authorized MAC address. This reads on detecting wireless interlopers (unauthorized users) and a single source address (MAC address). As can also been seen in the Abstract of the Harvey application, the purpose of the Harvey method and system is to detect the presence of unauthorized users (Harvey, Abstract). It is also noted that Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. For at least the reasons above, the rejection of the limitations is maintained.

7. As to Applicant's argument that, "Harvey et al. does not teach monitoring at least one signal characteristic for a plurality of signals from a device as part of an approach for profiling the signal characteristic of signals from a single source address, the with the specific intent of detecting wireless interlopers" (Remarks, p. 19), the Examiner respectfully disagrees. Applicant is directed to [0107-0108] of Harvey which specifically

mentions analyzing signals from the same MAC address to ensure that unauthorized users are not spoofing an authorized MAC address. This reads on detecting wireless interlopers (unauthorized users) and a single source address (MAC address). The system detects the physical locations of the signals which reads on a signal characteristic and if the physical locations of the signals from the same MAC address exceed a threshold, an alert is raised that an authorized user may be on the network. For at least the reasons above, the rejection of the limitations is maintained.

8. As to Applicant's argument that, "There is no teaching as to how this would be accomplished as part of monitoring at least one signal characteristic for a first signal of the plurality of signals fails to be commensurate with the monitored at least one signal characteristic for a second signal of the plurality of signals, particularly as to deciding the threshold characteristics that would not be sufficiently commensurate on these bases" (Remarks, p. 20), the Examiner respectfully disagrees. Applicant is directed to [0107-0108] of Harvey which specifically mentions analyzing signals from the same MAC address to ensure that unauthorized users are not spoofing an authorized MAC address. This reads on detecting wireless interlopers (unauthorized users) and a single source address (MAC address). The system detects the physical locations of the signals which reads on a signal characteristic and if the physical locations of the signals from the same MAC address exceed a threshold, an alert is raised that an authorized user may be on the network. For example, if two signals are received from the same MAC address simultaneously, but the geographical sources of these signals is such that it would be impossible for the same authorized device to transmit these signals, an alert

would be raised. For at least the reasons above, the rejection of the limitations is maintained.

9. As to Applicant's argument that, "Harvey et al. also does not teach such monitoring activities as part of an approach for profiling the signal characteristic of signals from a single source address, with the specific intent of detecting wireless interlopers" (Remarks, p. 20), the Examiner respectfully disagrees. Applicant is directed to [Abstract, 0107-0108] of Harvey which specifically mentions analyzing signals from the same MAC address to ensure that unauthorized users are not spoofing an authorized MAC address. This reads on detecting wireless interlopers (unauthorized users) and a single source address (MAC address). The system detects the physical locations of the signals which reads on a signal characteristic and if the physical locations of the signals from the same MAC address exceed a threshold, an alert is raised that an authorized user may be on the network. For at least the reasons above, the rejection of the limitations is maintained.

10. As to Applicant's argument that, "Harvey et al. also does not teach how such a bi-modal threshold would be determining as part of an approach for profiling the signal characteristic of signals from a single source address, with the specific intent of detecting wireless interlopers" (Remarks, p. 20), the Examiner respectfully disagrees. Applicant is directed to [0107-0108] of Harvey which specifically mentions analyzing signals from the same MAC address to ensure that unauthorized users are not spoofing an authorized MAC address. This reads on detecting wireless interlopers (unauthorized users) and a single source address (MAC address). The system detects the physical

locations of the signals which reads on a signal characteristic and if the physical locations of the signals from the same MAC address exceed a threshold, an alert is raised that an authorized user may be on the network. It is also noted that Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. For at least the reasons above, the rejection of the limitations is maintained.

11. As to Applicant's argument that, "Harvey et al. does not teach how such alerts are part of countering the wireless interloper, or the use of alerts as part of an approach for profiling the signal characteristics of signals from a single source address, with the specific intent of detecting wireless interlopers" (Remarks, p. 20), the Examiner respectfully disagrees. The Applicant is directed to Harvey [0122], "Once this illegal set of transitions has been identified, an alert could be raised so that an investigation could be conducted." An investigation reads on "countering the wireless interloper". As can also been seen in the Abstract of the Harvey application, the purpose of the Harvey method and system is to detect the presence of unauthorized users (Harvey, Abstract). For at least the reasons above, the rejection of the limitations is maintained.

12. As to Applicant's argument that, "Harvey et al. does not teach a monitoring action as part of an approach for profiling the signal characteristics of signals from a single source address, with the specific intent of detecting wireless interlopers" (Remarks, p. 21), the Examiner respectfully disagrees. Applicant is directed to [Abstract, 0107-0108] of Harvey which specifically mentions analyzing signals from the same MAC address to

ensure that unauthorized users are not spoofing an authorized MAC address. This reads on detecting wireless interlopers (unauthorized users) and a single source address (MAC address). The system detects the physical locations of the signals which reads on a signal characteristic and if the physical locations of the signals from the same MAC address exceed a threshold, an alert is raised that an authorized user may be on the network. For at least the reasons above, the rejection of the limitations is maintained.

13. As to Applicant's argument that, "Harvey et al. only teaches determining if remote locations are different or have changed, not that detecting that two sources for the plurality of signals that relate to the single source address if a discrepancy is determined to exist with regard to the monitored at least one signal characteristic for the plurality of signals" (Remarks, p. 21), the Examiner respectfully disagrees. Applicant is directed to [Abstract, 0107-0108] of Harvey which specifically mentions analyzing signals from the same MAC address to ensure that unauthorized users are not spoofing an authorized MAC address. This reads on detecting wireless interlopers (unauthorized users) and a single source address (MAC address). The system detects the physical locations of the signals which reads on a signal characteristic and if the physical locations of the signals from the same MAC address exceed a threshold, an alert is raised that an authorized user may be on the network. It is noted that in a spoofing attack, as described above, it is determined that there are two sources of the signals. The spoofer tries to hide the actual source by mimicking the address of an authorized user. For at least the reasons above, the rejection of the limitations is maintained.

14. As to Applicant's argument that, "while Harvey et al. may teach assessing changed locations for a device, this is not taught as part of an approach for profiling the signal characteristic of signals from a single source address, with the specific intent of detecting wireless interlopers" (Remarks, p. 21), the Examiner respectfully disagrees. Applicant is directed to [Abstract, 0107-0108] of Harvey which specifically mentions analyzing signals from the same MAC address to ensure that unauthorized users are not spoofing an authorized MAC address. This reads on detecting wireless interlopers (unauthorized users) and a single source address (MAC address). The system detects the physical locations of the signals which reads on a signal characteristic and if the physical locations of the signals from the same MAC address exceed a threshold, an alert is raised that an authorized user may be on the network. For at least the reasons above, the rejection of the limitations is maintained.

15. As to Applicant's argument that, "while Harvey et al. may teach the storing of address information, this is not taught as part of an approach for profiling the signal characteristic of signals from a single source address, with the specific intent of detecting wireless interlopers" (Remarks, p. 22), the Examiner respectfully disagrees. Applicant is directed to [Abstract, 0107-0108] of Harvey which specifically mentions analyzing signals from the same MAC address to ensure that unauthorized users are not spoofing an authorized MAC address. This reads on detecting wireless interlopers (unauthorized users) and a single source address (MAC address). The system detects the physical locations of the signals which reads on a signal characteristic and if the physical locations of the signals from the same MAC address exceed a threshold, an

alert is raised that an authorized user may be on the network. For at least the reasons above, the rejection of the limitations is maintained.

16. As to Applicant's argument that, "It would not have been obvious to a person of ordinary skill in the art to utilize Chesla's method of terminating communications because Chesla's methods are taught as part of a method of protecting a network from attack, not identifying wireless interlopers, as in the claimed methods" (Remarks, p. 23), the Examiner respectfully disagrees. The Examiner sees the unauthorized use of a network as an attack on the network and terminating the connection. It is also noted that there is no identifying step in the claimed methods. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the Harvey reference the security issues address not only the unauthorized use of the network, but the possible precursor to an attack (Harvey, [0012]). For at least the reasons above, the rejection of the limitations is maintained.

17. As to Applicant's argument that, "However, at the time the invention was made, it would not have been obvious to a person of ordinary skill in the art to adapt Chesla et al.'s approach of increasing packet tally at an ascertained value because Chesla's methods are taught as part of a method of protecting a network from attack, not

identifying wireless interlopers, as in the claimed methods" (Remarks, p. 23), the Examiner respectfully disagrees. The Examiner sees the unauthorized use of a network as an attack on the network. It is also noted that there is no identifying step in the claimed methods. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the Harvey reference the security issues address not only the unauthorized use of the network, but the possible precursor to an attack (Harvey, [0012]). For at least the reasons above, the rejection of the limitations is maintained.

18. As to Applicant's argument that, "However, at the time the invention was made, it would not have been obvious to a person of ordinary skill in the art to adapt Chesla et al.'s approach of determining if the bi-modal distribution is presented again; and if so, detecting the interloper with regard to the particular address based on the re-presentation of the bi-modal distribution, as the Chesla et al. methods are taught as part of a method of protecting a network from attack, not identifying wireless interlopers, as in the claimed methods" (Remarks, p. 24), the Examiner respectfully disagrees. The Examiner sees the unauthorized use of a network as an attack on the network. It is also noted that there is no identifying step in the claimed methods. In response to applicant's

argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the Harvey reference the security issues address not only the unauthorized use of the network, but the possible precursor to an attack (Harvey, [0012]). For at least the reasons above, the rejection of the limitations is maintained.

19. As to Applicant's argument that, "However, at the time the invention was made, it would not have been obvious to a person of ordinary skill in the art to adapt Chesla et al.'s approach of recording a payload of the packet, as the Chesla et al. methods are taught as part of a method of protecting a network from attack, not identifying wireless interlopers, as in the claimed methods" (Remarks, p. 25), the Examiner respectfully disagrees. The Examiner sees the unauthorized use of a network as an attack on the network. It is also noted that there is no identifying step in the claimed methods. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art.

See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the Harvey reference the security issues address not only the unauthorized use of the network, but the possible precursor to an attack (Harvey, [0012]). For at least the reasons above, the rejection of the limitations is maintained.

20. As to Applicant's argument that, "at the time the invention was made, it would not have been obvious to a person of ordinary skill in the art to adapt Bardsley's [methods] to the claimed methods, as Bardsley's methods are taught as part of a method of refusing a denial of service, not in identifying wireless interlopers, as in the claimed methods" (Remarks, p. 26), the Examiner respectfully disagrees. The Examiner sees the unauthorized use of a network as an attack on the network and a denial of service is a type of attack. It is also noted that there is no identifying step in the claimed methods. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the Harvey reference the security issues address not only the unauthorized use of the network, but the possible precursor to an attack (Harvey, [0012]). Harvey also specifically mentions identifying a denial of service attack as part of protecting a network from unauthorized

users (Harvey, [0015]). For at least the reasons above, the rejection of the limitations is maintained.

Response to Amendment

21. The Examiner has stated the below column and line numbers as examples. All columns and line numbers in the reference and the figures are relevant material and Applicant should take the entire reference into consideration upon the reply to this Office Action.

22. Claim 22 has been amended.

23. Claims 1-80 are pending.

Information Disclosure Statement

24. No Information Disclosure Statements have been submitted by the Applicant.

Claim Rejections - 35 USC § 112

25. In light of Applicant's amendment, the previous 35 USC § 112, 2nd paragraph rejection of claim 22 has been withdrawn.

Claim Rejections - 35 USC § 102

26. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

27. Claims 1-14, 16-33, 35-37, 49, 45-47, 50-53, 55, 58, 60-72 and 74-80 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent Application Publication 2004/0252837 to Harvey et al. (hereinafter Harvey).

With regards to claims 1, 13, 18-19, 22, 26, 29, 36-37, 39, 50-51, 55, 60, 62-63, 65, 68-69, 71, 75, Harvey teaches an apparatus comprising: at least one processor; and one or more media including processor-executable instructions that are capable of being executed by the at least one processor (Harvey, Figure 1, Figure 2), the processor-executable instructions adapted to direct the apparatus to perform actions comprising: monitoring at least one signal characteristic for a plurality of signals that relate to a single source address (Harvey, paragraph 0106, paragraph 0107, looks for characteristics for a particular MAC address); and detecting a wireless interloper if a discrepancy is determined to exist with regard to the monitored at least one signal characteristic for the plurality of signals (Harvey, paragraph 0107, location discrepancy).

With regards to claims 2, 16, 61, 74, 78, Harvey teaches the processor-executable instructions are adapted to cause the apparatus to perform further actions comprising: producing a plurality of communication beams; and receiving the plurality of signals via at least one communication beam of the plurality of communication beams (Harvey, paragraphs 0025-0029).

With regards to claims 3, 21, 28, 52, Harvey teaches the apparatus comprises an access station or a remote client (Harvey, paragraph 0026).

With regards to claims 4, 27, Harvey teaches the apparatus further comprises: an antenna array having a plurality of antenna elements; and a beam former coupled to the antenna array (Harvey, paragraph 0029).

With regards to claims 5, 32, Harvey teaches the monitoring action comprises: ascertaining the at least one signal characteristic for the plurality of signals (Harvey, paragraph 0107, location).

With regards to claims 6, 24-25, 30-31, 53, Harvey teaches the ascertaining action comprises: ascertaining the at least one signal characteristic as selected from the group comprising: arrival delay, arrival direction, multi-path offset, signal frequency, and signal strength (Harvey, paragraph 0042, signal strength, location triangulation for arrival direction).

With regards to claim 7, Harvey teaches the processor-executable instructions are adapted to cause the apparatus to perform a further action comprising: determining if the discrepancy exists with regard to the monitored at least one signal characteristic for the plurality of signals (Harvey, paragraph 0107, location discrepancy).

With regards to claims 8, 20, 64, 72, Harvey teaches the determining action comprises: determining if the monitored at least one signal characteristic for a first signal of the plurality of signals fails to be commensurate with the monitored at least one signal characteristic for a second signal of the plurality of signals (Harvey, paragraph 0042, 0107).

With regards to claim 9, Harvey teaches the determining action comprises: determining if a bi-modal distribution exists responsive to a predetermined threshold with regard to the monitored at least one signal characteristic for the plurality of signals (Harvey, paragraph 0107-0108).

With regards to claims 10, 14, 17, 45, 46, 58, 66, 70, 79-80, Harvey teaches everything described above and further teaches the processor-executable instructions are adapted to cause the apparatus to perform a further action comprising: if a wireless interloper is detected in the detecting action, countering the wireless interloper (Harvey, paragraphs 0122-0123, alerts raised to spoofing attacks).

With regards to claim 11, 67, Harvey teaches the monitoring action comprises: receiving a plurality of packets having the at least one signal characteristic, each packet of the plurality of packets including the single source address (Harvey, paragraph 0107, same MAC address).

With regards to claim 12, Harvey teaches the detecting action comprises: detecting that two sources exist for the plurality of signals that related to the single source address if a discrepancy is determined to exist with regard to the monitored at least one signal characteristic for the plurality of signals (Harvey, paragraphs 0122-0123, paragraphs 0106-0108).

With regards to claim 23, Harvey teaches the first characteristic and the at least one second characteristic being spatial (Harvey, paragraph 0107, location).

With regards to claims 33, 35, 47, 76-77, Harvey teaches storing the at least one characteristic for a packet in an entry of a table corresponding to a particular address (Harvey, paragraphs 0108, 0042, 0127).

Claim Rejections - 35 USC § 103

28. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

29. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

30. Claims 15, 34, 38, 40-41, 48-49, 54, 56, 59, 73 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Application Publication 2004/0252837 to Harvey et al (hereinafter Harvey) in view of US Patent Application Publication 2004/0250124 to Chesla et al. (hereinafter Chesla).

With regards to claims 15, 49, 59, Harvey teaches the action of countering comprises at least one action selected from the group comprising: providing notification of the detected wireless interloper (Harvey, paragraphs 0122-0123, alerts raised to

spoofing attacks); recording the ascertained at least one signal characteristic for the plurality of signals that relate to the single source address (Harvey, paragraphs 0108, 0042, 0127), but fails to teach terminating one or more communications that relate to the single source address. However, Chesla teaches terminating one or more communications that relate to the single source address (Chesla, paragraph 0426). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Chesla's method of terminating communications because it offers the advantage of blocking malicious traffic while minimizing the negative effects upon legitimate network traffic (Chesla, paragraph 0017).

With regards to claims 34, 38, 54, 56, 73, Harvey fails to teach increasing a packet tally at an ascertained value of the at least one characteristic at an entry corresponding to the particular address and the threshold comprising a number of packets. However, Chesla teaches increasing a packet tally at an ascertained value of the at least one characteristic at an entry corresponding to the particular address and the threshold comprising a number of packets (Chesla, paragraph 0033). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Chesla's method of counting packets because it offers the advantage of aiding in determining the existence of an attack and in determining if filtering countermeasures are effective (Chesla, paragraph 0032).

With regards to claims 40-41, Harvey fails to teach clearing the bi-modal distribution that exists with regard to the particular address; determining if the bi-modal distribution is presented again; and if so, detecting the interloper with regard to the particular address based on the re-presentation of the bi-modal distribution. However, Chesla teaches clearing the bi-modal distribution that exists with regard to the particular address; determining if the bi-modal distribution is presented again; and if so, detecting the interloper with regard to the particular address based on the re-presentation of the bi-modal distribution (Chesla, paragraph 0032-0033, detects intrusion, then filters, then restarts detection to determine if filters are effective). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Chesla's method of detection because it offers the advantage of blocking malicious traffic while minimizing the negative effects upon legitimate network traffic (Chesla, paragraph 0017).

With regards to claim 48, Harvey fails to teach recording a payload of the packet having the particular address. However, Chesla teaches recording a payload of the packet having the particular address (Chesla, paragraphs 0264-0265, records headers and payloads in buffers for analysis). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Chesla's method of detection because it offers the advantage of blocking malicious traffic while minimizing the negative effects upon legitimate network traffic (Chesla, paragraph 0017).

31. Claims 42, 43, 44, 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Application Publication 2004/0252837 to Harvey et al. (hereinafter Harvey) in view of US Patent No. 7,308,714 to Bardsley et al. (hereinafter Bardsley).

With regards to claims 42-44, 57, Harvey fails to teach applying an aging policy to logged characteristics for packets having the particular address. However, Bardsley teaches applying an aging policy to logged characteristics for packets having the particular address (Bardsley, column 5 lines 45-55, aging policy past 5 minutes). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Bardsley's method of using an aging policy because it offers the advantage of allowing fine tuning of attack signatures to allow detection of a signature of packets that occurs within a designated time window thus providing greater clarity of alerts to administrators (Bardsley, column 1 lines 30-50).

Conclusion

32. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to WILLIAM S. POWERS whose telephone number is (571)272-8573. The examiner can normally be reached on m-f 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/W. S. P./
Examiner, Art Unit 2434

William S. Powers
Examiner
Art Unit 2434

6/16/2010
/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434